Elementi di crittografia: La crittografia simmetrica

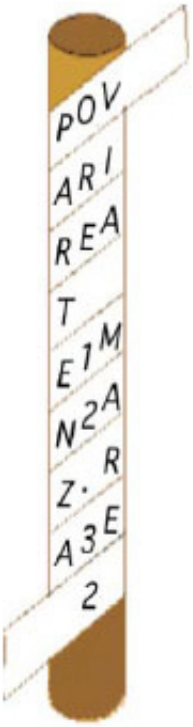
Nel precedente articolo abbiamo visto un caso particolare dell'applicazione della crittografia, ovvero l'hashing. Abbiamo visto quanto sia utile per la codifica di password o per assicurarci della validità di un file scaricato. Ma questa tecnica non è applicabile qualora fosse necessario codificare un messaggio che poi qualcuno dovrà leggere in quanto **l'hashing non è reversibile**.
Dovremo quindi affidarci alla crittografia simmetrica che, come la crittografia asimmetrica (la vedremo nel prossimo articolo), dovrà essere in grado di garantirci pricipalmente tre cose:

- **La confidenzialità**: solo il destinatario deve essere in grado di leggere il messaggio.
- **L'autenticità**: il destinatario deve essere certo che il mittente del messaggio sia veramente chi dice di essere.
- **L'integrità**: il messaggio, anche se impossibile da leggere, non deve poter essere modificato/corrotto da estranei senza che la cosa risulti immediatamente chiara.

Vediamo per iniziare alcuni esempi storici.

La crittografia simmetrica: una lunga storia

La necessità di rendere confidenziale un messaggio risale a migliaia di anni prima dell'invenzione dell'informatica. Le prime tecniche di crittografia delle quali si ha notizia, risalgono addirittura al nono secolo a.C. con il sistema della *scitala lacedemonica.* Consisteva nell'avvolgere ad elica un nastro di cuoio su di un cilindro . Quindi il messaggio veniva scritto in verticale. Una volta tolto il nastro dal cilindro era "impossibile" leggere il messaggio se non avvolgendolo su di un cilindro dello stesso diametro.



Nel corso della storia troviamo poi molti esempi, alcuni dei quali veramente sbalorditivi, come *enigma*, la codificatrice meccanica a rotori inventata ed utilizzata dai nazisti nella seconda guerra mondiale per crittografare i messaggi destinati ai sommergibili.

Le migliori menti dell’epoca furono radunate a Bletchley Park in Inghilterra per crecare di decifrare i messaggi scritti con questa macchina, ma ebbero dei successi solo parziali e non riuscirono comunque a svelare fino in fondo il meccanismo di codifica.

Troviamo anche esempi piuttosto banali, come il cifrario di Cesare che consiste semplicemente in un numero, che rappresenta lo scostamento delle lettere (il cifrario originale prevedeva uno scostamento di 3).

NBVSLALP

Non é altro che MAURIZIO sostituendo ogni lettera con quella successiva (la chiave di codifica é quindi 1).

> Curiosità: il primo caso di pubblicità occulta lo troviamo nel film 2001 odissea nello spazio di Kubrick dove il nome del super-computer HAL 9000 diventa in realtà IBM applicando il cifrario di Cesare con chiave -1.

Come puoi vedere, il principio della crittografia simmetrica consiste nel disporre di **un'unica chiave con la quale si codifica e si decodifica il messaggio** (il diametro del cilindro, il posizionamento dei rotori di enigma, il numero di scostamento delle lettere nel cifrario di Cesare).

E' come se immaginassimo di mettere il nostro messaggio in un baule che dispone di una serratura; io ho una chiave ed il ricevente ha la stessa chiave. Quando avrà tra le mani il baule, il ricevente potrà aprirlo con la sua chiave (uguale alla mia, per questo si chiama crittografia simmetrica). In questo modo viene garantita l'**autenticità** (se il baule era chiuso, posso averlo chiuso solo io) e la **confidenzialità** (nessun altro oltre me ed il ricevente dispone delle chiavi).
Rimane il problema dell'**integrità**.
Se il mio baule contenesse una videocassetta e fosse accidentalmente o intenzionalmente fatto passare attraverso un forte campo magnetico?
Il problema dell'integrità ha molto a che vedere con gli algoritmi di hashing che abbiamo trattato nel precedente articolo e vedremo in seguito come.

Chiaramente, nella realtà, dovremo codificare delle stringhe, e lo faremo attraverso delle funzioni che generalmente passano almeno tre parametri

- La stringa da codificare.
- La chiave di codifica.
- La modalità (codifica o decodifica).

Queste funzioni fanno capo a degli algoritmi molto complessi dei quali non ci occuperemo.
Vediamo invece un esempio di codifica simmetrica di un messaggio.
PHP mette a disposizione diverse funzioni appartenenti alle librerie mcrypt.

Vediamo dunque un esempio di codifica attraverso PHP.
Utilizzeremo la funzione mcrypt_cfb() che come puoi vedere passa quattro parametri.

1. L'agoritmo di cifratura. Ecco la lista degli algoritmi supportati.
2. La chiave di cifratura.
3. La stringa da cifrare.
4. La modalità (MCRYPT_ENCRYPT o MCRYPT_DECRYPT).

Quindi potremmo agire in questo modo

Per ottenere questo:

ãñòÏ#ðzz|qòÓ¦|

In realtà otterremo anche un errore di livello *Warnig* in quanto il quinto parametro, dato per opzionale, è fortemente raccomandato ed è il vettore di inizializzazione dell'algoritmo, sul quale non intendo soffermarmi, quello che mi interessa ora è il principio.

Ricevendo questo messaggio e conoscendo la chiave (e l'algoritmo), non dovrò fare altro che agire in questo modo

per ottenere come risultato:

Frase da cifrare

Conclusione

Il limite evidente della crittografia simmetrica é la **necessità di disporre di una chiave concordata tra le due persone che si scambiano il messaggio**. E' ovvio che questa tecnica, nell'era dell'informatica moderna, non é sufficiente.
Immagina se per codificare i dati della tua carta di credito, quando li trasmetti per eseguire un acquisto online, dovessi utilizzare la crittografia simmetrica. Si dovrebbe richiedere una chiave al gestore della transazione per poter codificare i dati, ma come verrebbe codificato il messaggio contenete la chiave? Dovrebbe esserti inviato per posta?
Sarebbe veramente troppo complicato, mentre l'acquisto online deve essere semplice, veloce.

Nel prossimo articolo vedremo come questo limite venga superato dalla **crittogafia asimmetrica** grazie alla quale non abbiamo nessuna necessità di concordare le chiavi di cifratura. Ma vedremo anche perché, nonostante questo, la crittografia simmetrica non sia per nulla superata.
Hai mai utilizzato degli algoritmi simmetrici? A quale scopo?